PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326695
(43)Date of publication of application : 22.11.2001

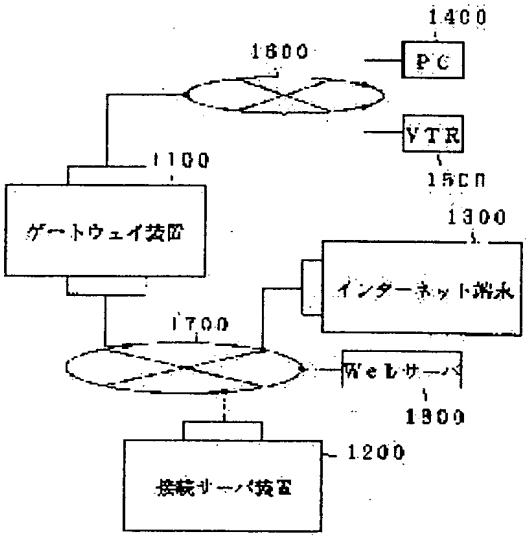
(51)Int.Cl. H04L 12/66
G06F 13/00
H04L 12/28
H04L 12/56

(21)Application number : 2000-146256
(22)Date of filing : 18.05.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TAKEDA HIDETOSHI

(54) GATEWAY UNIT, CONNECTION SERVER UNIT, INTERNET TERMINAL, NETWORK SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a gateway unit that interconnects a private network and the Internet, and relieves the load of complicated processings for maintaining security.
SOLUTION: An Internet terminal 1300, connected to the Internet 1700, communicates with a PC 1400 or a VTR 1500 as a private terminal. A connection server unit 1200 connected to the Internet authenticates the communication to the private network 1600. The gateway unit 1100 receives only an encrypted packet, received from the connection server unit 1200, to maintain security of the private network 1600 and to reduce the processing load of the gateway unit 1100 to a low level.



LEGAL STATUS

[Date of request for examination] 16.04.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－326695
（P2001－326695A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.'		識別記号	FI		テーマコード(参考)
H04L	12/66		G06F 13/00	351Z	5B089
G06F	13/00	351	H04L 11/20	B	5K030
H04L	12/28		11/00	310D	5K033
	12/56		11/20	102A	

審査請求　未請求　請求項の数26　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－146256(P2000－146256)

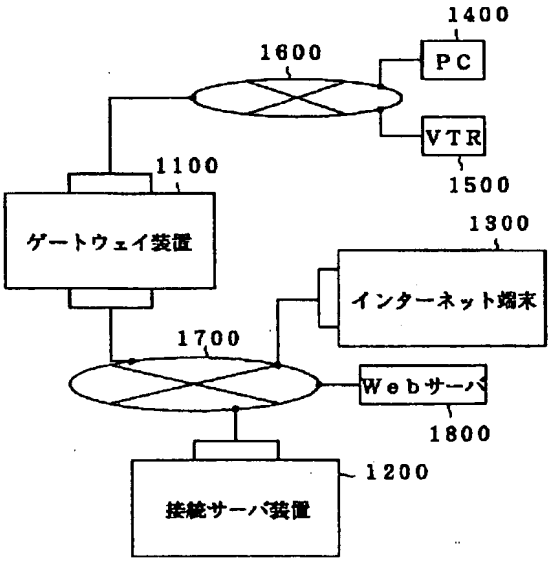
(22)出願日　平成12年５月18日(2000.5.18)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　武田　英俊
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100084364
弁理士　岡本　宜喜

Ｆターム(参考)　5B089 GA31 HA10 KA17 KB06 KB13 KC52 KC58 KH30
5K030 GA15 HD03 HD06 HD09 JA05 JT02
5K033 AA08 CB02 CB09 CC01 DA06 DB18

(54)【発明の名称】　ゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステム

(57)【要約】
【課題】　プライベート・ネットワークとインターネットを相互に接続するゲートウェイ装置において、セキュリティを維持するための複雑な処理を軽減すること。
【解決手段】　インターネット１７００に接続されたインターネット端末１３００から、プライベート端末装置としてＰＣ１４００又はＶＴＲ１５００と通信する。このときプライベート・ネットワーク１６００への通信を行うための認証を、インターネットに接続された接続サーバ装置１２００で行う。ゲートウェイ装置１１００は接続サーバ装置１２００から受け取る暗号化されたパケットのみを受信することで、プライベート・ネットワーク１６００のセキュリティを保ち、且つゲートウェイ装置１００の処理負担を小さくすることができる。



【特許請求の範囲】
【請求項１】　プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、
前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、
前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、
前記インターネットからパケットを受信する第２のパケット受信手段と、
前記インターネットに対してパケットを送信する第２のパケット送信手段と、
前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、
前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行って前記第２のパケット送信手段に与えると共に、前記第２のパケット受信手段又は前記暗号解読手段から入力されたパケットのアドレス及びプロトコルの変換を行って前記第１のパケット送信手段に与えるパケット変換手段と、を具備し、
前記第２のパケット受信手段は、
暗号化されたパケットを受信した場合に暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、
前記暗号解読手段は、
暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするゲートウェイ装置。
【請求項２】　前記パケット変換手段は、
代理サーバ機能を持ち、前記プライベート・ネットワークから受け取ったパケットの発信元ＩＰアドレスとして前記インターネットで使用する単一のＩＰアドレスを付加して出力することを特徴とする請求項１記載のゲートウェイ装置。
【請求項３】　前記暗号解読手段は、
前記インターネットに接続され、予め決められた接続サーバ装置のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項１記載のゲートウェイ装置。
【請求項４】　前記パケット変換手段は、
前記パケット変換手段によって変換し、前記プライベート端末装置に対して送信したパケットに対する応答として前記プライベート端末装置から出力された応答パケット、及び前記暗号解読手段から出力されたパケットのみを受け取ることを特徴とする請求項３記載のゲートウェイ装置。
【請求項５】　前記パケット変換手段は、
前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第１のパケット送信手段に与えることを特徴とする請求項１～４のいずれか１項記載のゲートウェイ装置。
【請求項６】　前記パケット変換手段は、
前記第２のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のＩＰアドレスを含む応答パケットを前記第２のパケット送信手段に出力することを特徴とする請求項３～５のいずれか１項記載のゲートウェイ装置。
【請求項７】　前記パケット変換手段は、
Ｗｅｂサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Ｗｅｂサーバによって処理し、処理の結果によって生成したパケットを前記第１のパケット送信手段に与えることを特徴とする請求項１～６のいずれか１項記載のゲートウェイ装置。
【請求項８】　プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、
前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、
前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、
前記インターネットからパケットを受信する第２のパケット受信手段と、
前記インターネットに対してパケットを送信する第２のパケット送信手段と、
パケットのデータ部分を暗号化した暗号化パケットを前記第２のパケット送信手段に与える暗号化手段と、
前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、
前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行ったパケットを前記暗号化手段に出力すると共に、前記暗号解読手段から受け取ったパケットのアドレス及びプロトコルの変換を行って前記第１のパケット送信手段に与えるパケット変換手段と、を具備し、
前記第２のパケット受信手段は、
受信したパケットを前記暗号解読手段に与え、
前記暗号解読手段は、
暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするゲートウェイ装置。
【請求項９】　前記パケット変換手段は、
前記第１のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして、前記暗号化手段に与えることを特徴とする請求項８記載のゲートウェイ装置。
【請求項１０】　前記暗号解読手段は、
前記インターネットに接続され、予め決められた接続サーバ装置のＩＰアドレスを送信元としたパケットを入力

し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項８記載のゲートウェイ装置。

【請求項１１】　前記パケット変換手段は、
前記第１のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして前記暗号化手段に出力し、
前記暗号解読手段は、
前記接続サーバ装置のＩＰアドレスを送信元としたパケットを対象とし、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項８記載のゲートウェイ装置。

【請求項１２】　前記パケット変換手段は、
前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第１のパケット送信手段に与えると共に、前記第１のパケット受信手段から受け取ったパケットをデータ部分に含み、前記接続サーバ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とする請求項１１記載のゲートウェイ装置。

【請求項１３】　前記パケット変換手段は、
前記第２のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のＩＰアドレスを含む応答パケットを前記第２のパケット送信手段に与えることを特徴とする請求項９～１２のいずれか１項記載のゲートウェイ装置。

【請求項１４】　プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、
前記インターネットからパケットを受信するパケット受信手段と、
前記インターネットに対してパケットを送信するパケット送信手段と、
前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、
パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、
前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備することを特徴とする接続サーバ装置。

【請求項１５】　前記パケット変換手段は、
前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とする請求項１４記載の接続サーバ装置。

【請求項１６】　前記認証手段は、
認証結果として認証ＩＤを出力し、
前記パケット変換手段は、
前記認証手段が出力する前記認証ＩＤ、及び前記パケット受信手段から受け取るパケットに含まれる認証ＩＤを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とする請求項１４又は１５記載の接続サーバ装置。

【請求項１７】　プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、
前記インターネットからパケットを受信するパケット受信手段と、
前記インターネットに対してパケットを送信するパケット送信手段と、
前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、
パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、
前記パケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、
前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記パケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備し、
前記パケット受信手段は、
データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、
前記暗号解読手段は、
暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とする接続サーバ装置。

【請求項１８】　前記暗号解読手段は、
前記ゲートウェイ装置のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とする請求項１７記載の接続サーバ装置。

【請求項１９】　前記パケット変換手段は、
前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットを送信パケットとして前記パケット送信手段に与えると共に、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェ

イ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とする請求項１７記載の接続サーバ装置。
【請求項２０】　前記パケット変換手段は、
代理サーバ機能を持ち、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットの発信元ＩＰアドレスとして、前記接続サーバ装置のＩＰアドレスを付加して出力することを特徴とする請求項１９記載の接続サーバ装置。
【請求項２１】　前記認証手段は、
認証結果として認証ＩＤを出力し、
前記パケット変換手段は、
前記認証手段が出力する前記認証ＩＤ、及び前記パケット受信手段から受け取るパケットに含まれる認証ＩＤを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とする請求項１７～２０のいずれか１項記載の接続サーバ装置。
【請求項２２】　前記パケット変換手段は、
Ｗｅｂサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Ｗｅｂサーバによって処理し、処理の結果によって生成したパケットを前記第１のパケット送信手段に与えることを特徴とする請求項１７～２１のいずれか１項記載の接続サーバ装置。
【請求項２３】　インターネットに接続され、プライベート・ネットワークに接続されたプライベート端末機器との間で通信を行うインターネット端末であって、
前記インターネットからパケットを受信するパケット受信手段と、
前記インターネットに対してパケットを送信するパケット送信手段と、
前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、
前記接続サーバ装置から前記パケット受信手段を介して認証結果を受け取り、前記接続サーバ装置に対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記パケット送信手段に与えるパケット生成手段と、を具備することを特徴とするインターネット端末。
【請求項２４】　前記認証要求手段は、
前記接続サーバ装置から認証結果として認証ＩＤを受け取り、前記認証ＩＤを前記パケット生成手段に与えることを特徴とする請求項２３記載のインターネット端末。
【請求項２５】　プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、
前記ゲートウェイ装置は、
前記プライベートネットワークと前記インターネットの両者に接続され、
前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、
前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、
前記インターネットからパケットを受信する第２のパケット受信手段と、
前記インターネットに対してパケットを送信する第２のパケット送信手段と、
前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、
前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第２のパケット送信手段に与えると共に、前記第２のパケット受信手段から出力されたパケット又は前記暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第１のパケット送信手段に与える第１のパケット変換手段と、を具備するものであり、
前記接続サーバ装置は、
前記インターネットに接続され、
前記インターネットからパケットを受信する第３のパケット受信手段と、
前記インターネットに対してパケットを送信する第３のパケット送信手段と、
前記第３のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第３のパケット送信手段に与える認証手段と、
パケットのデータ部分を暗号化した暗号化パケットを前記パケット送信手段に与える暗号化手段と、
前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行って前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与える第２のパケット変換手段と、を具備するものであり、
前記インターネット端末は、
前記インターネットからパケット受信する第４のパケット受信手段と、
前記インターネットに対してパケットを送信する第４のパケット送信手段と、
前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、

前記接続サーバ装置から前記第４のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第４のパケット送信手段に与えるパケット生成手段と、を具備するものであることを特徴とするネットワークシステム。

【請求項２６】　プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、

前記ゲートウェイ装置は、

前記プライベートネットワークと前記インターネットの両者に接続され、

前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、

前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、

前記インターネットからパケットを受信する第２のパケット受信手段と、

前記インターネットに対してパケットを送信する第２のパケット送信手段と、

パケットのデータ部分を暗号化した暗号化パケットを前記第２のパケット送信手段に与える第１の暗号化手段と、

前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第１の暗号解読手段と、

前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第１の暗号化手段に与えると共に、前記第１の暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第１のパケット送信手段に与える第１のパケット変換手段と、を具備するものであり、

前記接続サーバ装置は、

前記インターネットに接続され、

前記インターネットからパケットを受信する第３のパケット受信手段と、

前記インターネットに対してパケットを送信する第３のパケット送信手段と、

前記第３のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第３のパケット送信手段に与える認証手段と、

パケットのデータ部分を暗号化した暗号化パケットを前記第３のパケット送信手段に与える暗号化手段と、

前記第３のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第２の暗号解読手段と、

前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記第３のパケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行ったものを変換パケットとして前記ゲートウェイ装置宛のパケットとして出力する際に、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記第２の暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットをそのまま変換パケットに変換する共に、前記第２の暗号解読手段から出力されたパケットを変換パケットに変換する第２のパケット変換手段と、を具備するものであり、

前記インターネット端末は、

前記インターネットからパケット受信する第４のパケット受信手段と、

前記インターネットに対してパケットを送信する第４のパケット送信手段と、

前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、

前記接続サーバ装置から前記第４のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第４のパケット送信手段に与えるパケット生成手段と、を具備するものであることを特徴とするネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、プライベート・ネットワークとインターネットとを相互に接続するための技術に係わり、特にゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムに関する。

【０００２】

【従来の技術】これまで、プライベート・ネットワーク（イントラネット）とインターネットを接続する場合、両方のネットワークが接続される位置にゲートウェイ装置を設置し、パケットを相互に転送することで２つのネットワークを相互接続していた。このようなゲートウェイ装置はルータとも呼ばれることもある。しかしながら、パケットを相互に転送するだけのゲートウェイ装置では、インターネットから、プライベート・ネットワークに接続されたプライベート端末装置に対して自由にアクセスができるため、不特定のユーザから不正なアクセスを受けてしまう危険性があった。

【０００３】このような不正なアクセスを防止し、プライベート・ネットワークのセキュリティを確保するためには、プライベート・ネットワークとインターネットと

の間にゲートウェイ装置を接続する場合、パケットそのまま転送せず、ファイア・ウォールと呼ばれる機能を設けることが多い。このようなファイア・ウォールでは、インターネットからプライベート・ネットワークに接続されたプライベート端末装置に対してパケットを直接に転送しないようにすることで、プライベート・ネットワークのセキュリティを確保することができる。

【0004】一方、ゲートウェイ装置では、代理サーバ（プロキシ・サーバ）機能を持つことによって、プライベート・ネットワークに接続されたプライベート端末装置から、インターネットに接続されたＷｅｂサーバ等へのアクセスを可能にすることができる。このような代理サーバは、プライベート・ネットワークに接続されたプライベート端末装置に対してＷｅｂサーバとして動作し、プライベート端末装置から受け取った要求を自らの要求としてインターネットに送信する。そしてこの要求の結果、インターネットを介して受け取った応答を、プライベート・ネットワーク内の要求を行ったプライベート端末装置に転送する。

【0005】プライベート・ネットワークとインターネットの両方に接続された代理サーバがこのような動作を行うことで、プライベート・ネットワークとインターネットとの間で直接パケットの転送を行わなくても、プライベート・ネットワークからインターネットのＷｅｂサーバへのアクセスが実現できる。なお、この代理サーバの機能はIETF（The Internet Engineering Task Force）のRFC（Request for Comments）2616 Hypertext Transfer Protocol 1.1で定められている。

【0006】またこのようなファイア・ウォールでは、インターネットからプライベート・ネットワークへのアクセスを行う場合、ゲートウェイ装置においてインターネットに接続された端末やユーザの認証を行い、認証の結果許可された端末及びユーザが発信したパケットのみを転送するようにしている。このようなパケットの転送機能によって、不特定のユーザからの不正なアクセスを防ぐことができる。

【0007】一方、複数のプライベート・ネットワーク同士を、インターネットを介して相互に接続する仮想プライベート・ネットワーク（VPN: Virtual Private Network）が知られている。この仮想プライベート・ネットワークでは、プライベート・ネットワークとインターネットを接続するゲートウェイ装置において、プライベート・ネットワーク内のパケットを、インターネットを介して別のゲートウェイ装置に転送する。これを受けた別のゲートウェイ装置は、受信したパケットをプライベート・ネットワークに送信する。

【0008】例えば２つのプライベート・ネットワーク、即ちネットワーク１とネットワーク２があり、それぞれゲートウェイ１とゲートウェイ２を介してインターネットに接続されていたとする。ネットワーク１に接続された端末からネットワーク２に接続されたサーバにパケットを送信する場合、このパケットはまずゲートウェイ１に送られる。ゲートウェイ１は、パケットの宛先アドレスからサーバがネットワーク２に接続された装置であると判断し、受信したパケットを、インターネットを介してゲートウェイ２に向けて送信する。一方これを受信したゲートウェイ２は、受信したパケットをサーバに対して送信する。

【0009】このように仮想プライベート・ネットワークでは、複数のゲートウェイ装置がインターネットを介してパケットの転送を行うことで、複数のプライベート・ネットワーク同士が相互に接続されているのと同等の効果を得ることができる。なお、仮想プライベート・ネットワークの詳細に関しては、例えばIETFのRFC2764A Framework for IP Based Virtual Private Networkに記載されている。

【0010】

【発明が解決しようとする課題】従来、セキュリティを確保した上でプライベート・ネットワークとインターネットを接続する場合、上述のような代理サーバ機能によってプライベート・ネットワークからインターネットへの通信を可能にする一方で、インターネットからプライベート・ネットワークへのパケットの転送を制限したり、また事前に認証を行うといった方法を用いていた。

【0011】しかしながら、高いセキュリティを保った上でインターネットからプライベート・ネットワークへのアクセスを可能にするためには、ゲートウェイ装置において複雑な認証手順を設定したり、またインターネットから要求を受け付けるためのサーバ機能が必要となる。このような機能を実現することは、例えば家庭内などの小規模なプライベート・ネットワークをインターネットに接続するゲートウェイ装置では、大きな負担となってしまうという課題があった。

【0012】本発明は、このような従来の問題点に鑑みてなされたものであって、ゲートウェイ装置の負担を軽減しつつ、プライベート・ネットワークのセキュリティを確保し、かつインターネットからプライベート・ネットワークに接続されたプライベート端末装置へのアクセスを可能にするゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムを夫々実現することを目的とする。

【0013】

【課題を解決するための手段】本願の請求項１の発明は、プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、前記インターネットからパケットを受信する第２のパケット受信手段と、前記イン

ターネットに対してパケットを送信する第２のパケット送信手段と、前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行って前記第２のパケット送信手段に与えると共に、前記第２のパケット受信手段又は前記暗号解読手段から入力されたパケットのアドレス及びプロトコルの変換を行って前記第１のパケット送信手段に与えるパケット変換手段と、を具備し、前記第２のパケット受信手段は、暗号化されたパケットを受信した場合に暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするものである。

【００１４】本願の請求項２の発明は、請求項１のゲートウェイ装置において、前記パケット変換手段は、代理サーバ機能を持ち、前記プライベート・ネットワークから受け取ったパケットの発信元ＩＰアドレスとして前記インターネットで使用する単一のＩＰアドレスを付加して出力することを特徴とするものである。

【００１５】本願の請求項３の発明は、請求項１のゲートウェイ装置において、前記暗号解読手段は、前記インターネットに接続され、予め決められた接続サーバ装置のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【００１６】本願の請求項４の発明は、請求項３のゲートウェイ装置において、前記パケット変換手段は、前記パケット変換手段によって変換し、前記プライベート端末装置に対して送信したパケットに対する応答として前記プライベート端末装置から出力された応答パケット、及び前記暗号解読手段から出力されたパケットのみを受け取ることを特徴とするものである。

【００１７】本願の請求項５の発明は、請求項１～４のいずれか１項のゲートウェイ装置において、前記パケット変換手段は、前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第１のパケット送信手段に与えることを特徴とするものである。

【００１８】本願の請求項６の発明は、請求項３～５のいずれか１項のゲートウェイ装置において、前記パケット変換手段は、前記第２のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のＩＰアドレスを含む応答パケットを前記第２のパケット送信手段に出力することを特徴とするものである。

【００１９】本願の請求項７の発明は、請求項１～６のいずれか１項のゲートウェイ装置において、前記パケット変換手段は、Ｗｅｂサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Ｗｅｂサーバによって処理し、処理の結果によって生成したパケットを前記第１のパケット送信手段に与えることを特徴とするものである。

【００２０】本願の請求項８の発明は、プライベート端末装置が接続されたプライベート・ネットワークとインターネットとを接続するゲートウェイ装置であって、前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、前記インターネットからパケットを受信する第２のパケット受信手段と、前記インターネットに対してパケットを送信する第２のパケット送信手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第２のパケット送信手段に与える暗号化手段と、前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行ったパケットを前記暗号化手段に出力すると共に、前記暗号解読手段から受け取ったパケットのアドレス及びプロトコルの変換を行って前記第１のパケット送信手段に与えるパケット変換手段と、を具備し、前記第２のパケット受信手段は、受信したパケットを前記暗号解読手段に与え、前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするものである。

【００２１】本願の請求項９の発明は、請求項８のゲートウェイ装置において、前記パケット変換手段は、前記第１のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして、前記暗号化手段に与えることを特徴とするものである。

【００２２】本願の請求項１０の発明は、請求項８のゲートウェイ装置において、前記暗号解読手段は、前記インターネットに接続され、予め決められた接続サーバ装置のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【００２３】本願の請求項１１の発明は、請求項８のゲートウェイ装置において、前記パケット変換手段は、前記第１のパケット受信手段から受け取ったパケットを、前記インターネットに接続されて予め決められた接続サーバ装置宛のパケットとして前記暗号化手段に出力し、前記暗号解読手段は、前記接続サーバ装置のＩＰアドレスを送信元としたパケットを対象とし、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【００２４】本願の請求項１２の発明は、請求項１１のゲートウェイ装置において、前記パケット変換手段は、

前記暗号解読手段から受け取ったパケットのデータ部分を送信パケットとして前記第１のパケット送信手段に与えると共に、前記第１のパケット受信手段から受け取ったパケットをデータ部分に含み、前記接続サーバ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とするものである。

【００２５】本願の請求項１３の発明は、請求項９～１２のいずれか１項のゲートウェイ装置において、前記パケット変換手段は、前記第２のパケット受信手段を介して前記接続サーバ装置の問い合わせパケットを受け取った場合、前記接続サーバ装置のＩＰアドレスを含む応答パケットを前記第２のパケット送信手段に与えることを特徴とするものである。

【００２６】本願の請求項１４の発明は、プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信するパケット送信手段と、前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備することを特徴とするものである。

【００２７】本願の請求項１５の発明は、請求項１４の接続サーバ装置において、前記パケット変換手段は、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とするものである。

【００２８】本願の請求項１６の発明は、請求項１４又は１５の接続サーバ装置において、前記認証手段は、認証結果として認証ＩＤを出力し、前記パケット変換手段は、前記認証手段が出力する前記認証ＩＤ、及び前記パケット受信手段から受け取るパケットに含まれる認証ＩＤを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とするものである。

【００２９】本願の請求項１７の発明は、プライベート・ネットワークに接続されたゲートウェイ装置とインターネットを介して通信を行う接続サーバ装置であって、前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信するパケット送信手段と、前記パケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記パケット送信手段に与える認証手段と、パケットのデータ部分を暗号化して前記パケット送信手段に与える暗号化手段と、前記パケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記パケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行った変換パケットを前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与えるパケット変換手段と、を具備し、前記パケット受信手段は、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットを前記パケット変換手段に与え、前記暗号解読手段は、暗号の解読を行ったパケットを前記パケット変換手段に与えることを特徴とするものである。

【００３０】本願の請求項１８の発明は、請求項１７の接続サーバ装置において、前記暗号解読手段は、前記ゲートウェイ装置のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力することを特徴とするものである。

【００３１】本願の請求項１９の発明は、請求項１７の接続サーバ装置において、前記パケット変換手段は、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットを送信パケットとして前記パケット送信手段に与えると共に、前記パケット受信手段から受け取ったパケットをデータ部分に含み、前記ゲートウェイ装置宛のパケットを生成して前記暗号化手段に与えることを特徴とするものである。

【００３２】本願の請求項２０の発明は、請求項１９の接続サーバ装置において、前記パケット変換手段は、代理サーバ機能を持ち、前記暗号解読手段から受け取ったパケットのデータ部分に含まれるパケットの発信元ＩＰアドレスとして、前記接続サーバ装置のＩＰアドレスを付加して出力することを特徴とするものである。

【００３３】本願の請求項２１の発明は、請求項１７～２０のいずれか１項の接続サーバ装置において、前記認証手段は、認証結果として認証ＩＤを出力し、前記パケット変換手段は、前記認証手段が出力する前記認証ＩＤ、及び前記パケット受信手段から受け取るパケットに含まれる認証ＩＤを比較することによって、前記インターネット端末が認証されているか否かを判断し、認証結果が一致する場合にパケット変換することを特徴とするものである。

【００３４】本願の請求項２２の発明は、請求項１７～

２１のいずれか１項の接続サーバ装置において、前記パケット変換手段は、Ｗｅｂサーバ機能を持ち、前記暗号化手段から受け取ったパケットを前記Ｗｅｂサーバによって処理し、処理の結果によって生成したパケットを前記第１のパケット送信手段に与えることを特徴とするものである。

【００３５】本願の請求項２３の発明は、インターネットに接続され、プライベート・ネットワークに接続されたプライベート端末機器との間で通信を行うインターネット端末であって、前記インターネットからパケットを受信するパケット受信手段と、前記インターネットに対してパケットを送信するパケット送信手段と、前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、前記接続サーバ装置から前記パケット受信手段を介して認証結果を受け取り、前記接続サーバ装置に対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記パケット送信手段に与えるパケット生成手段と、を具備することを特徴とするものである。

【００３６】本願の請求項２４の発明は、請求項２３のインターネット端末において、前記認証要求手段は、前記接続サーバ装置から認証結果として認証ＩＤを受け取り、前記認証ＩＤを前記パケット生成手段に与えることを特徴とするものである。

【００３７】本願の請求項２５の発明は、プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、前記ゲートウェイ装置は、前記プライベートネットワークと前記インターネットの両者に接続され、前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、前記インターネットからパケットを受信する第２のパケット受信手段と、前記インターネットに対してパケットを送信する第２のパケット送信手段と、前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する暗号解読手段と、前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第２のパケット送信手段に与えると共に、前記第２のパケット受信手段から出力されたパケット又は前記暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第１のパケット送信手段に与える第１のパケット変換手段と、を具備するものであり、前記接続サーバ装置は、前記インターネットに接続され、前記インターネットからパケットを受信する第３のパケット受信手段と、前記インターネットに対してパケットを送信する第３のパケット送信手段と、前記第３のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第３のパケット送信手段に与える認証手段と、パケットのデータ部分を暗号化した暗号化パケットを前記パケット送信手段に与える暗号化手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行って前記ゲートウェイ装置宛のパケットとして前記暗号化手段に与える第２のパケット変換手段と、を具備するものであり、前記インターネット端末は、前記インターネットからパケット受信する第４のパケット受信手段と、前記インターネットに対してパケットを送信する第４のパケット送信手段と、前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、前記接続サーバ装置から前記第４のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第４のパケット送信手段に与えるパケット生成手段と、を具備することを特徴とするものである。

【００３８】本願の請求項２６の発明は、プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するネットワークシステムであって、前記ゲートウェイ装置は、前記プライベートネットワークと前記インターネットの両者に接続され、前記プライベート・ネットワークからパケットを受信する第１のパケット受信手段と、前記プライベート・ネットワークに対してパケットを送信する第１のパケット送信手段と、前記インターネットからパケットを受信する第２のパケット受信手段と、前記インターネットに対してパケットを送信する第２のパケット送信手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第２のパケット送信手段に与える第１の暗号化手段と、前記第２のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第１の暗号解読手段と、前記第１のパケット受信手段で受信したパケットに含まれる前記プライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを前記第１の暗号化手段に与えると共に、前記第１の暗号解読手段から出力された暗号解読済のパケットに対して、アドレス及びプロトコルの変換を行ったパケットを前記第１のパケット送信手段に与える第１のパケット

変換手段と、を具備するものであり、前記接続サーバ装置は、前記インターネットに接続され、前記インターネットからパケットを受信する第３のパケット受信手段と、前記インターネットに対してパケットを送信する第３のパケット送信手段と、前記第３のパケット受信手段を介して前記インターネットに接続されたインターネット端末から認証の要求を受け取って前記インターネット端末の認証を行い、認証結果を前記第３のパケット送信手段に与える認証手段と、パケットのデータ部分を暗号化した暗号化パケットを前記第３のパケット送信手段に与える暗号化手段と、前記第３のパケット受信手段で受信したパケットの少なくともデータ部分を解読する第２の暗号解読手段と、前記認証手段によって認証された前記インターネット端末から、前記プライベート・ネットワークに接続されたプライベート端末機器への転送を求めるパケットを前記第３のパケット受信手段を介して受け取り、アドレス及びプロトコルの変換を行ったものを変換パケットとして前記ゲートウェイ装置宛のパケットとして出力する際に、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを前記第２の暗号解読手段に与え、暗号化されていないパケットを受信した場合に非暗号化パケットをそのまま変換パケットに変換する共に、前記第２の暗号解読手段から出力されたパケットを変換パケットに変換する第２のパケット変換手段と、を具備するものであり、前記インターネット端末は、前記インターネットからパケット受信する第４のパケット受信手段と、前記インターネットに対してパケットを送信する第４のパケット送信手段と、前記プライベート・ネットワークに接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置に対して問い合わせを行い、前記接続サーバ装置に対して自己の端末の認証要求を行う認証要求手段と、前記接続サーバ装置から前記第４のパケット受信手段を介して認証結果を受け取り、前記接続サーバに対して前記プライベート・ネットワークへの転送を要求するパケットを生成して前記第４のパケット送信手段に与えるパケット生成手段と、を具備することを特徴とするものである。

【００３９】

【発明の実施の形態】（実施の形態１）本発明の実施の形態１におけるゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムについて、図１～図４を用いて説明する。図１は本実施の形態において、インターネット、プライベート・ネットワーク、ゲートウェイ装置、接続サーバ装置、インターネット端末、Ｗｅｂサーバ、プライベート端末等の接続形態を示す説明図である。

【００４０】プライベート・ネットワーク１６００にはプライベート端末装置として例えばＰＣ１４００、ＶＴＲ１５００が接続されている。このプライベート・ネットワーク１６００はゲートウェイ装置１１００を介してインターネット１７００に接続されている。インターネット１７００には接続サーバ装置１２００、インターネット端末１３００、Ｗｅｂサーバ１８００などが接続されている。

【００４１】プライベート・ネットワーク１６００は家庭内の機器同士を接続しているネットワークである。ゲートウェイ装置１１００は、プライベート・ネットワーク１６００とインターネット１７００の両方に接続され、パケットの相互変換を行うものである。

【００４２】ゲートウェイ装置１１００は図２に示すように、第１のパケット送信手段１１０１、第１のパケット受信手段１１０２、暗号解読手段１１０３、第１のパケット変換手段１１０４、第２のパケット受信手段１１０５、第２のパケット送信手段１１０６を含んで構成される。

【００４３】第１のパケット受信手段１１０２はプライベート・ネットワーク１６００からパケットを受信するものである。第１のパケット送信手段１１０１はプライベート・ネットワーク１６００に対してパケットを送信するものである。第２のパケット受信手段１１０５はインターネット１７００からパケットを受信するものである。第２のパケット送信手段１１０６はインターネット１７００に対してパケットを送信するものである。暗号解読手段１１０３は、第２のパケット受信手段１１０５で受信した暗号化パケットの少なくともデータ部分を解読すると共に、インターネット１７００に接続され、予め決められた接続サーバ装置１２００のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力するものである。

【００４４】パケット変換手段１１０４は、第１のパケット受信手段１１０２で受信したパケットに含まれるプライベート端末装置のアドレス及びプロトコルの変換を行った変換パケットを第２のパケット送信手段１１０６に与えると共に、第２のパケット受信手段１１０５又は暗号解読手段１１０３から入力されたパケットのアドレス及びプロトコルの変換を行って第１のパケット送信手段１１０１に与えるものである。またパケット変換手段１１０４は、第２のパケット受信手段１１０５を介して接続サーバ装置１２００の問い合わせパケットを受け取った場合、接続サーバ装置１２００のＩＰアドレスを含む応答パケットを第２のパケット送信手段１１０６に出力する。

【００４５】また接続サーバ装置１２００は図３に示すように、第３のパケット送信手段１２０１、第３のパケット受信手段１２０２、暗号化手段１２０３、認証手段１２０４、第２のパケット変換手段１２０５を含んで構成される。

【００４６】パケット受信手段１２０２はインターネット１７００からパケットを受信するものである。パケッ

ト送信手段１２０１はインターネット１７００に対してパケットを送信するものである。認証手段１２０４はパケット受信手段１２０２を介してインターネット１７００に接続されたインターネット端末１３００から認証の要求を受け取って、インターネット端末１３００の認証を行い、認証結果を認証ＩＤとして出力し、パケット送信手段１２０１に与えるものである。暗号化手段１２０３はパケットのデータ部分を暗号化してパケット送信手段１２０１に与えるものである。

【００４７】パケット変換手段１２０５は、認証手段１２０４によって認証されたインターネット端末１３００から、プライベート・ネットワーク１６００に接続されたプライベート端末装置への転送を求めるパケットを受け取り、アドレス及びプロトコルの変換を行った変換パケットをゲートウェイ装置１１００宛のパケットとして暗号化手段１２０３に与えるものである。またパケット変換手段１２０５は、認証手段１２０４が出力する認証ＩＤ、及びパケット受信手段１２０２から受け取るパケットに含まれる認証ＩＤを比較することによって、インターネット端末１３００が認証されているか否かを判断し、認証結果が一致する場合にパケット変換するものとする。

【００４８】インターネット端末１３００は、インターネット１７００を介してプライベート端末装置との間でパケットの通信を行うもので、図４に示すように第４のパケット送信手段１３０１、第４のパケット受信手段１３０２、パケット生成手段１３０３、認証要求手段１３０４を含んで構成される。

【００４９】パケット受信手段１３０２はインターネット１７００からパケットを受信するものである。パケット送信手段１３０１はインターネット１７００に対してパケットを送信するものである。認証要求手段１３０４は、プライベート・ネットワーク１６００に接続されたプライベート端末機器と通信を行うため、パケットの転送を行う接続サーバ装置１２００に対して問い合わせを行い、接続サーバ装置１２００に対して自己の端末の認証要求を行うものである。パケット生成手段１３０３は接続サーバ装置１２００からパケット受信手段１３０２を介して認証結果を受け取り、接続サーバ装置１２００に対してプライベート・ネットワーク１６００への転送を要求するパケットを生成してパケット送信手段１３０１に与えるものである。

【００５０】まず、プライベート・ネットワーク１６００に接続されたプライベート端末装置であるＰＣ１４００が、インターネット１７００に接続されたＷｅｂサーバ１８００との間で通信を行う場合について以下に説明する。例えばここで行う通信とは、ホームページの閲覧などに伴う通信である。

【００５１】ＰＣ１４００はＷｅｂサーバ１８００に対して送るべきパケットを、プライベート・ネットワーク１６００を介して先ずゲートウェイ装置１１００に送信する。ゲートウェイ装置１１００の第１のパケット受信手段１１０２はこのパケットを受信し、パケット変換手段１１０４に出力する。パケット変換手段１１０４はこのパケットのＩＰアドレスを付け替えた変換パケットを第２のパケット送信手段１１０６に出力する。第２のパケット送信手段１１０６はパケット変換手段１１０４から受け取ったパケットをインターネット１７００を介してＷｅｂサーバ１８００に送信する。

【００５２】一方、第２のパケット受信手段１１０５が、上記のようにしてＷｅｂサーバ１８００に送ったパケットに対する応答を含む応答パケットを受け取った場合、このパケットをパケット変換手段１１０４に与える。パケット変換手段１１０４は、このパケットのＩＰアドレスを付け替えてＰＣ１４００に送信するために、第１のパケット送信手段１１０１に出力する。第１のパケット送信手段１１０１から送信されたこの応答を含むパケットは、プライベート・ネットワーク１６００を介してＰＣ１４００に到達する。以上のような動作によって、ＰＣ１４００がインターネット１７００に接続されたＷｅｂサーバ１８００との間で通信を行うことができる。

【００５３】ここでパケット変換手段１１０４が行うＩＰアドレスの付け替えや、応答を含むパケットの転送機能は、プロキシー（代理）サーバ機能と呼ばれている（IETFRFC 2616 Hypertext Transfer Protocol 1.1 参照）。ゲートウェイ装置１１００がこのような代理サーバ機能を持っている場合、ＰＣ１４００はインターネット１７００に接続されたＷｅｂサーバ１８００に対して送信するパケットを、ゲートウェイ装置１１００に送信すればよい。ゲートウェイ装置１１００は、プライベート端末装置から受け取ったパケットの発信元ＩＰアドレスを、ゲートウェイ装置１１００のインターネット１７００におけるアドレスに付け替えて、すなわちゲートウェイ装置１１００自身が発信するパケットとして、目的のＷｅｂサーバ１８００に送信する。そして、このようにして送信したパケットに対する応答含むパケットをゲートウェイ装置１１００が受け取ると、再びＩＰアドレスの付け替えを行って、この応答を含むパケットをプライベート・ネットワーク１６００を介してプライベート端末装置に送信する。

【００５４】ゲートウェイ装置１１００がこのような代理サーバ機能を持つことによって、プライベート・ネットワーク１６００に接続されたプライベート端末装置はインターネット１７００に接続されたＷｅｂサーバ１８００との間で通信を行うことができ、結果としてホームページの閲覧ができる。

【００５５】なお、送信したパケットに対する応答を含むパケットの識別は、ＴＣＰ／ＩＰの通信で用いられるポート番号によって行うことができる。ゲートウェイ装

置１１００がＷｅｂサーバ１８００に送信したパケットには、パケット変換手段１１０４によって指定されたポート番号が含まれおり、この送信パケットに対応した応答を含むパケットにも、ここで指定したポート番号が含まれている。このため、パケット変換手段１１０４は、Ｗｅｂサーバ１８００のＩＰアドレスとポート番号を確認することで、送信済みのどのパケットに対する応答であるかを識別することができる。

【００５６】次に、インターネット１７００に接続されたインターネット端末１３００が、プライベート・ネットワーク１６００に接続されたＶＴＲ１５００との間で通信を行う場合について以下に説明する。このような通信とは、インターネット１７００に接続されたインターネット端末１３００から、ＶＴＲ１５００の動作制御や状態問い合わせ等を行う場合である。

【００５７】インターネット端末１３００の認証要求手段１３０４は、ＶＴＲ１５００への通信に先だって、まずゲートウェイ装置１１００に対して接続サーバ装置の問い合わせ要求を行う。インターネット端末１３００の認証要求手段１３０４は、この問い合わせ要求を含むパケットをパケット送信手段１３０１に与える。パケット送信手段１３０１はこのパケットをインターネット１７００を介して、ゲートウェイ装置１１００の第２のパケット受信手段１１０５に送信する。第２のパケット受信手段１１０５がこの問い合わせを含むパケットを受信すると、パケット変換手段１１０４に与える。パケット変換手段１１０４はこの問い合わせに対する応答として、接続サーバ装置１２００のＩＰアドレスを含むパケットを第２のパケット送信手段１１０６に与える。第２のパケット送信手段１１０６はこの応答を含むパケットをインターネット端末１３００に送信する。インターネット端末１３００のパケット受信手段１３０２は、このパケットを受信して認証要求手段１３０４に出力する。

【００５８】次に認証要求手段１３０４は、上記の問い合わせによってＩＰアドレスを受け取った接続サーバ装置１２００に対して、認証要求を含むパケットを出力する。インターネット端末１３００のパケット送信手段１３０１によって送信された認証要求を含むパケットは、インターネット１７００を介して接続サーバ装置１２００のパケット受信手段１２０２によって受信される。接続サーバ装置１２００のパケット受信手段１２０２は、この認証要求を含むパケットを認証手段１２０４に与える。認証手段１２０４がこのパケットを受け取ると、予め定められた方法によって認証要求を検査し、ＶＴＲ１５００との間での通信を許可できるか否かを判断する。なおここで行う認証の判断は、例えばインターネット端末１３００が予め登録されたものであるか否か、またパスワードや暗証番号の確認等によって行うことができる。また、認証の方法によっては複数のパケットの送受信を伴う場合もある。

【００５９】この判断の結果、認証手段１２０４はインターネット端末１３００に対してＶＴＲ１５００との間の通信を許可する場合には、認証の結果として認証ＩＤを含むパケットを出力し、通信を許可しない場合には認証の失敗を示すパケットを出力し、パケット送信手段１２０１に与える。パケット送信手段１２０１は、このパケットをインターネット１７００に送信する。インターネット端末１３００のパケット受信手段１３０２がこのパケット受信すると、認証要求手段１３０４に与える。

【００６０】上記のような認証手続きの結果、インターネット端末１３００がＶＴＲ１５００との間の通信を許可された場合、パケット生成手段１３０３はＶＴＲ１５００に送信するパケットに加えて、認証要求手段１３０４から受け取る認証ＩＤおよび接続サーバ装置１２００のＩＰアドレスを使用して、ＶＴＲ１５００に対しての転送を要求するパケットを生成してパケット送信手段１３０１に出力する。パケット送信手段１３０１はこのパケットをインターネット１７００を介して接続サーバ装置１２００に送信する。

【００６１】接続サーバ装置１２００のパケット受信手段１２０２は、インターネット端末１３００によって送信されたＶＴＲ１５００への転送を要求するパケットを受信し、これをパケット変換手段１２０５に与える。パケット変換手段１２０５は、パケット受信手段１２０２から受け取ったパケットに含まれる認証ＩＤと、インターネット端末１３００のＩＰアドレスとを認証手段１２０４から受け取ると、通信を許可した端末の認証ＩＤとＩＰアドレスとの組み合わせと比較し、このパケットが認証手段１２０４によって通信が許可されたものであるか否かを確認する。そして許可されているパケットの場合には、受け取ったパケットをデータ部分に含むパケットを新たに生成し、暗号化手段１２０３に与える。このようなパケットのデータ部分に別のパケットを含めて通信する方法は、パケットのカプセル化と呼ばれている。

【００６２】暗号化手段１２０３は、受け取ったパケットのデータ部分を、予めゲートウェイ装置１１００との間で決められた方法によって暗号化した暗号化パケットをパケット送信手段１２０１に与える。パケット送信手段１２０１はこの暗号化パケットをインターネット１７００を介してゲートウェイ装置１１００に送信する。

【００６３】ゲートウェイ装置１１００の第２のパケット受信手段１１０５が暗号化パケットを受信すると、このパケットを暗号解読手段１１０３に与える。暗号解読手段１１０３は、接続サーバ装置１２００から送信されたパケットのみを受け取り、接続サーバ装置１２００との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段１１０４に出力される。一方、暗号の解読が正常に行われなかったパケット、及び接続サーバ装置１２００以外から受け取ったパケットは破棄される。

【００６４】パケット変換手段１１０４は前述の代理サーバに相当する機能を持ち、暗号解読手段１１０３から受け取ったパケットのデータ部分から、カプセル化されたパケットを取り出し、ＩＰアドレスの付け替え等を行って第１のパケット送信手段１１０１に与える。第１のパケット送信手段１１０１は、このパケットをゲートウェイ装置１１００が発信するパケットとして、プライベート・ネットワーク１６００を介してＶＴＲ１５００に送信する。

【００６５】ＶＴＲ１５００は、ゲートウェイ装置１１００によって送信されたパケットを受信すると、この受信パケットに対する応答を含むパケットをゲートウェイ装置１１００に送信する。ゲートウェイ装置１１００の第１のパケット受信手段１１０２は受信したパケットをパケット変換手段１１０４に与える。パケット変換手段１１０４はＩＰアドレスの付け替え等を行った変換パケットを第２のパケット送信手段１１０６に与える。第２のパケット送信手段１１０６はこのパケットをインターネット１７００を介してインターネット端末１３００に送信する。

【００６６】このようにして、インターネット１７００に接続されたインターネット端末１３００と、プライベート・ネットワークに接続されたＶＴＲ１５００との間での通信が可能となる。即ちインターネット端末１３００がＶＴＲ１５００の動作制御等を行うことができる。これにより、例えば家の外から、家庭内にあるＶＴＲの録画予約、予約状況の確認等を行うことができる。

【００６７】以上のように接続サーバ装置１２００がインターネット端末１３００の認証を行い、またゲートウェイ装置１１００は接続サーバ装置１２００から送信されたパケットのみを受信することで、接続サーバ装置１２００において高いセキュリティを実現し、ゲートウェイ装置１１００の処理負荷を軽減することができる。こうしてインターネット１７００からプライベート・ネットワーク１６００へのアクセスが可能となる。ここで、セキュリティの強さは接続サーバ装置１２００の認証手段１２０４によって決まるものであり、必要に応じて新しく又は強固なものに更新することができる。このため、ゲートウェイ装置１１００の置き換えや、機能の更新等を行うことなく、ゲートウェイ装置１１００及びプライベート・ネットワーク１６００のセキュリティの強化が実現される。

【００６８】更に接続サーバ装置１２００は、ゲートウェイ装置１１００と同等の機能を有する他の複数のゲートウェイ装置に対して同様の機能を発揮することができる。このような場合、接続サーバ装置１２００のセキュリティを強化することで、多数のゲートウェイ装置及びプライベート・ネットワークのセキュリティを強化することが可能となり、個々のゲートウェイ装置のセキュリティを強化する場合に比べて、効率的かつ迅速な対応が可能となる。

【００６９】なお、インターネット端末１３００が、予め接続サーバ装置１２００のＩＰアドレスを知っていれば、ゲートウェイ装置１１００に対して接続先の問い合わせを行わずに、接続サーバ装置１２００に対して直接認証要求を行うことができる。またこのような場合、ゲートウェイ装置１１００のインターネット１７００側のＩＰアドレスが動的な割り当てにより変化する場合でも、上記と同等の機能を実現することが可能となる。更には、ゲートウェイ装置１１００のＩＰアドレスがインターネット１７００に接続された他の機器に知られることがないため、より高いセキュリティの実現できる。

【００７０】上記のような夫々の装置の動作に加えて、ゲートウェイ装置１１００のパケット変換手段１１０４がＷｅｂサーバ機能を有する場合、インターネット端末１３００によって送信されたパケットをＶＴＲ１５００に転送するのではなく、このＷｅｂサーバがパケットを処理し、その結果生成されたパケットをＶＴＲ１５００に送信することもできる。このような場合、インターネット端末１３００は、パケット変換手段１１０４のＷｅｂサーバにアクセスしてＶＴＲ１５００に要求する動作に対応する入力や選択等を行う。このＷｅｂサーバは入力パケットを処理し、ＶＴＲ１５００への動作制御を行うためのパケットを生成し、第１のパケット送信手段１１０１を介してＶＴＲ１５００に送信する。またＶＴＲ１５００から送信された応答は、パケット変換手段１１０４のＷｅｂサーバによって受け取られる。Ｗｅｂサーバはウｅｂページの更新を行うことによって、ＶＴＲ１５００から受け取った応答をインターネット端末１３００に提示することができる。

【００７１】なお、プライベート・ネットワークに接続されたプライベート端末機器とインターネットに接続されたインターネット端末との間の通信を、接続サーバ装置とゲートウェイ装置とを介して実現するシステムを、ネットワークシステムと呼ぶ。

【００７２】このようにゲートウェイ装置１１００のパケット変換手段１１０４がＷｅｂサーバ機能を持つことによって、インターネット端末１３００はＶＴＲ１５００の動作制御を直接行う必要がなくなる。この場合、インターネット端末１３００には、ＶＴＲ１５００を制御するための専用のソフトウェアを用意しなくても、汎用のブラウザ等によってＶＴＲ１５００の動作を制御することができる。

【００７３】（実施の形態２）次に本発明の実施の形態２におけるゲートウェイ装置、接続サーバ装置、インターネット端末、ネットワークシステムについて、図５～図８を用いて説明する。図５は本実施の形態において、インターネット、プライベート・ネットワーク、ゲートウェイ装置、接続サーバ装置、インターネット端末、Ｗｅｂサーバ、プライベート端末等の接続形態を示す説明

図である。

【００７４】プライベート・ネットワーク２６００にはプライベート端末装置として、例えばＰＣ２４００、ＶＴＲ２５００が接続されている。このプライベート・ネットワーク２６００はゲートウェイ装置２１００を介してインターネット２７００に接続されている。インターネット２７００には接続サーバ装置２２００、インターネット端末２３００、Ｗｅｂサーバ２８００などが接続されている。

【００７５】プライベート・ネットワーク２６００は家庭内の機器同士を接続しているネットワークである。ゲートウェイ装置２１００は、プライベート・ネットワーク２６００とインターネット２７００の両方に接続され、パケットの相互変換を行うものである。

【００７６】ゲートウェイ装置２１００は図６に示すように、第１のパケット送信手段２１０１、第１のパケット受信手段２１０２、第１の暗号解読手段２１０３、第１のパケット変換手段２１０４、第１の暗号化手段２１０５、第２のパケット受信手段２１０６、第２のパケット送信手段２１０７を含んで構成される。

【００７７】第１のパケット受信手段２１０２はプライベート・ネットワーク２６００からパケットを受信するものである。第１のパケット送信手段２１０１はプライベート・ネットワーク２６００に対してパケットを送信するものである。第２のパケット受信手段２１０６はインターネット２７００からパケットを受信するものである。第２のパケット送信手段２１０７はインターネット２７００に対してパケットを送信するものである。

【００７８】暗号化手段２１０５はパケットのデータ部分を暗号化し、暗号化パケットを第２のパケット送信手段２１０７に与えるものである。暗号解読手段２１０３は第２のパケット受信手段２１０６で受信したパケットの少なくともデータ部分を解読するものである。尚、暗号解読手段２１０３は、インターネット２７００に接続され、予め決められた接続サーバ装置２２００のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力するものとする。

【００７９】パケット変換手段２１０４は、第１のパケット受信手段２１０２で受信したパケットに含まれるプライベート端末装置のアドレス及びプロトコルの変換を行ったパケットを暗号化手段２１０５に出力すると共に、暗号解読手段２１０３から受け取ったパケットのアドレス及びプロトコルの変換を行って第１のパケット送信手段２１０１に与えるものである。またパケット変換手段２１０４は、第１のパケット受信手段２１０２から受け取ったパケットを、インターネット２７００に接続されて予め決められた接続サーバ装置２２００宛のパケットとして、暗号化手段２１０５に与える。更にパケット変換手段２１０４は、第２のパケット受信手段２１０６を介して接続サーバ装置２２００の問い合わせパケットを受け取った場合、接続サーバ装置２２００のＩＰアドレスを含む応答パケットを第２のパケット送信手段２１０７に与えるものとする。

【００８０】次に接続サーバ装置２２００は図７に示すように、第３のパケット送信手段２２０１、第３のパケット受信手段２２０２、第２の暗号化手段２２０３、認証手段２２０４、第２の暗号解読手段２２０５、第２のパケット変換手段２２０６を含んで構成される。

【００８１】パケット受信手段２２０２はインターネット２７００からパケットを受信するものである。パケット送信手段２２０１はインターネット２７００に対してパケットを送信するものである。認証手段２２０４は、パケット受信手段２２０２を介して、インターネット２７００に接続されたインターネット端末２３００から認証の要求を受け取って、インターネット端末２３００の認証を行い、認証結果をパケット送信手段２２０１に与えるものである。

【００８２】暗号化手段２２０３はパケットのデータ部分を暗号化してパケット送信手段２２０１に与えるものである。暗号解読手段２２０５はパケット受信手段２２０２で受信したパケットの少なくともデータ部分を解読するものである。尚、暗号解読手段２２０５は、ゲートウェイ装置２１００のＩＰアドレスを送信元としたパケットを入力し、且つ正常に暗号の解読を行ったパケットのみを出力するものとする。

【００８３】パケット変換手段２２０６は、認証手段２２０４によって認証されたインターネット端末２３００から、プライベート・ネットワーク２６００に接続されたプライベート端末機器への転送を求めるパケットを、パケット受信手段２２０２を介して受け取り、アドレス及びプロトコルの変換を行った変換パケットをゲートウェイ装置２１００宛のパケットとして暗号化手段２２０３に与えるものである。尚、パケット変換手段２２０６は、代理サーバ機能を持ち、暗号解読手段２２０５から受け取ったパケットのデータ部分に含まれるパケットの発信元ＩＰアドレスとして、接続サーバ装置２２００のＩＰアドレスを付加して出力するものとする。そしてパケット変換手段２２０６は認証手段２２０４が出力する認証ＩＤ、及びパケット受信手段２２０２から受け取るパケットに含まれる認証ＩＤを比較することによって、インターネット端末２３００が認証されているか否かを判断し、認証結果が一致する場合にパケット変換する。

【００８４】尚、パケット受信手段２２０２は、データ部分の暗号化されたパケットを受信した場合には暗号化パケットを暗号解読手段２２０５に与え、暗号化されていないパケットを受信した場合に非暗号化パケットをパケット変換手段２２０６に与えるものとする。

【００８５】インターネット端末２３００は、インターネット２７００を介してプライベート端末装置であるＰＣ２４００やＶＴＲ２５００との間でパケットの通信を

行うもので、図8に示すように第4のパケット送信手段２３０１、第4のパケット受信手段２３０２、パケット生成手段２３０３、認証要求手段２３０４を含んで構成される。これらの構成要素と各構成要素の機能は、実施の形態1と同様であるので、説明を省略する。

【００８６】まず、プライベート端末装置であるＰＣ２４００が、インターネット２７００に接続されたＷｅｂサーバ２８００との間で通信を行う場合について以下に説明する。ここで行う通信とは、例えばホームページの閲覧などに伴う通信である。

【００８７】ＰＣ２４００は、Ｗｅｂサーバ２８００に対して送るべきパケットを、先ずプライベート・ネットワーク２６００を介してゲートウェイ装置２１００に送信する。ゲートウェイ装置２１００の第1のパケット受信手段２１０２はこのパケットを受信すると、パケット変換手段２１０４に与える。パケット変換手段２１０４は受け取ったパケットをデータ部分に含むパケットを生成し、変換パケットに変換して暗号化手段２１０５に与える。このように、パケットのデータ部分に別のパケットを含めて通信する方法は、パケットのカプセル化と呼ばれている。

【００８８】暗号化手段２１０５は受け取ったパケットのデータ部分を、接続サーバ装置２２００との間で予め定められた方法で暗号化して暗号化パケットを生成し、第2のパケット送信手段２１０７に与える。第2のパケット送信手段２１０７は、暗号化手段２１０５から受け取った暗号化パケットをインターネット２７００を介して接続サーバ装置２２００に送信する。

【００８９】接続サーバ装置２２００のパケット受信手段２２０２は、暗号化パケットを受信して暗号解読手段２２０５に与える。暗号解読手段２２０５はゲートウェイ装置２１００から送信されたパケットのみを受け取り、ゲートウェイ装置２１００との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段２２０６に出力され、暗号の解読が正常に行われなかったパケット、及びゲートウェイ装置２１００以外から受け取ったパケットは破棄される。

【００９０】パケット変換手段２２０６は、暗号の解読されたパケットのデータ部分から、ゲートウェイ装置２１００がＰＣ２４００から受信した形式のパケットを取り出す。またパケット変換手段２２０６は、実施の形態1におけるゲートウェイ装置１１００のパケット変換手段１１０４と同様に代理サーバ機能を持つ。即ち、暗号解読手段２２０５から受け取ったパケットのデータ部分より取り出したパケットに対して、ＩＰアドレスの付け替えを行い、パケット送信手段２２０１に与える。パケット送信手段２２０１は、受け取ったパケットをインターネット２７００を介してＷｅｂサーバ２８００に送信する。

【００９１】一方、接続サーバ装置２２００のパケット受信手段２２０２が、上記のようにしてＷｅｂサーバ２８００に送ったパケットに対する応答を含む応答パケットを受け取ると、パケット受信手段２２０２はこの応答パケットをパケット変換手段２２０６に与える。パケット変換手段２２０６は代理サーバの機能によるＩＰアドレスを付け替え等を行い、このパケットをデータ部分に含むパケットを生成して暗号化手段２２０３に与える。暗号化手段２２０３は、受け取ったパケットのデータ部分を、ゲートウェイ装置２１００との間で予め定められた方法で暗号化し、暗号化パケットをパケット送信手段２２０１に与える。パケット送信手段２２０１はこの暗号化パケットをインターネット２７００を介してゲートウェイ装置２１００に送信する。

【００９２】ゲートウェイ装置２１００の第2のパケット受信手段２１０６は、上記の暗号化パケットを受信して暗号解読手段２１０３に与える。暗号解読手段２１０３は接続サーバ装置２２００から送信されたパケットのみを受け取り、接続サーバ装置２２００との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段２１０４に出力され、暗号の解読が正常に行われなかったパケット、及び接続サーバ装置２２００以外から受け取ったパケットは破棄される。

【００９３】パケット変換手段２１０４は、暗号解読手段２１０３から受け取ったパケットのデータ部分に含まれるパケットを取り出して、第1のパケット送信手段２１０１に与える。第1のパケット送信手段２１０１はこのパケットをプライベート・ネットワーク１６００を介してＰＣ２４００に送信する。

【００９４】以上のような動作によって、ＰＣ２４００がインターネット２７００に接続されたＷｅｂサーバ２８００との間で通信を行うことができ、結果としてＷｅｂサーバ２８００に備えられたホームページの閲覧などが行える。

【００９５】次に、インターネット２７００に接続されたインターネット端末２３００が、プライベート・ネットワーク２６００に接続されたＶＴＲ２５００との間で通信を行う場合について以下に説明する。このような通信とは、例えばインターネット２７００に接続されたインターネット端末装置２３００から、ＶＴＲ２５００の動作制御や状態問い合わせ等を行うものである。

【００９６】インターネット端末２３００の認証要求手段２３０４は、ＶＴＲ２５００への通信に先だって、まずゲートウェイ装置２１００に対して接続サーバ装置の問い合わせ要求を行う。この問い合わせ要求を含むパケットは、インターネット端末２３００のパケット送信手段２３０１によって、インターネット２７００を介してゲートウェイ装置２１００の第2のパケット受信手段２１０６に送信される。第2のパケット受信手段２１０６

がこの問い合わせを含むパケットを受信すると、このパケットをパケット変換手段２１０４に与える。パケット変換手段２１０４はこの問い合わせに対する応答として、接続サーバ装置２２００のＩＰアドレスを含む応答パケットを第２のパケット送信手段２１０７に与える。第２のパケット送信手段２１０７はこの応答パケットをインターネット端末２３００に送信する。インターネット端末２３００のパケット受信手段２３０２はこのパケットを受信して認証要求手段２３０４に与える。

【００９７】次に認証要求手段２３０４は、上記の問い合わせによってＩＰアドレスを受け取った接続サーバ装置２２００に対して、認証要求を含むパケットを出力する。認証要求を含むパケットがインターネット２７００を介して接続サーバ装置２２００のパケット受信手段２２０２によって受信されると、パケット受信手段２２０２は、この認証要求を含むパケットを認証手段２２０４に与える。認証手段２２０４はこのパケットを受け取ると、この認証要求を予め定められた方法によって検査し、ＶＴＲ２５００との間での通信を許可できるか否かを判断する。尚、ここで行う認証の判断は、例えばインターネット端末２３００が予め登録されたものであるか否か、又はパスワードや暗証番号の確認等によって行うことができる。また、認証の方法によっては、複数のパケットの送受信を伴う場合もある。

【００９８】この判断の結果、認証手段２２０４はインターネット端末２３００にＶＴＲ２５００との間の通信を許可する場合には、認証の結果として認証ＩＤを含むパケットをパケット送信手段２２０１に与え、通信を許可しない場合には認証の失敗を示すパケットをパケット送信手段２２０１に与える。パケット送信手段２２０１はこのパケットをインターネット２７００に送信する。インターネット端末２３００のパケット受信手段２３０２がこのパケットを受信すると、認証要求手段２３０４に与える。

【００９９】上記のような認証手続きの結果、インターネット端末２３００がＶＴＲ２５００との間の通信を許可された場合、パケット生成手段２３０３はＶＴＲ２５００に送信するパケットに加えて、認証要求手段２３０４から受け取る認証ＩＤおよび接続サーバ装置２２００のＩＰアドレスを使用して、ＶＴＲ２５００に対しての転送を要求するパケットを生成し、パケット送信手段２３０１に与える。パケット送信手段２３０１はこのパケットをインターネット２７００を介して接続サーバ装置２２００に送信する。

【０１００】接続サーバ装置２２００のパケット受信手段２２０２は、インターネット端末２３００から送信されたＶＴＲ２５００への転送を要求するパケットを受信すると、このパケットをパケット変換手段２２０６に与える。

【０１０１】パケット変換手段２２０６は、パケット受信手段２２０２から受け取ったパケットに含まれる認証ＩＤとインターネット端末２３００のＩＰアドレスを、認証手段２２０４から受け取り、通信を許可した端末の認証ＩＤ及びＩＰアドレスとの組み合わせを比較する。そして、このパケットが認証手段２２０４によって通信が許可されたものであるか否かを確認する。この確認によって許可されているパケットの場合には、代理サーバの機能によるＩＰアドレスを付け替え等を行い、このパケットをデータ部分に含む変換パケットを生成し、暗号化手段２２０３に与える。

【０１０２】暗号化手段２２０３は、受け取ったパケットのデータ部分を、ゲートウェイ装置２１００との間で予め定められた方法で暗号化し、暗号化パケットをパケット送信手段２２０１に与える。パケット送信手段２２０１はこの暗号化パケットをインターネット２７００を介してゲートウェイ装置２１００に送信する。

【０１０３】ゲートウェイ装置２１００の第２のパケット受信手段２１０６がこの暗号化されたパケットを受信すると、このパケットを暗号解読手段２１０３に与える。暗号解読手段２１０３は接続サーバ装置２２００から送信されたパケットのみを受け取り、接続サーバ装置２２００との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段２１０４に出力され、暗号の解読が正常に行われなかったパケット、及び接続サーバ装置２２００以外から受け取ったパケットは破棄される。

【０１０４】パケット変換手段２１０４は、暗号解読手段２１０３から受け取ったパケットのデータ部分に含まれるパケットを取り出して、第１のパケット送信手段２１０１に出力する。第１のパケット送信手段２１０１はこのパケットをプライベート・ネットワーク２６００を介して、ＶＴＲ２５００に送信する。

【０１０５】ＶＴＲ２５００はゲートウェイ装置２１００によって送信されたパケットを受信すると、このパケットに対する応答を含む応答パケットをゲートウェイ装置２１００に送信する。ゲートウェイ装置２１００の第１のパケット受信手段２１０２は、受信した応答パケットをパケット変換手段２１０４に与える。パケット変換手段２１０４は、受け取ったパケットをデータ部分に含む変換パケットを生成し、暗号化手段２１０５に与える。

【０１０６】暗号化手段２１０５は、受け取ったパケットのデータ部分を、接続サーバ装置２２００との間で予め定められた方法で暗号化し、暗号化パケットを第２のパケット送信手段２１０７に与える。第２のパケット送信手段２１０７は、暗号化手段２１０５から受け取った暗号化パケットをインターネット２７００を介して接続サーバ装置２２００に対して送信する。

【０１０７】接続サーバ装置２２００のパケット受信手段２２０２は、上記の暗号化されたパケットを受信して

暗号解読手段２２０５に与える。暗号解読手段２２０５はゲートウェイ装置２１００から送信されたパケットのみを受け取り、ゲートウェイ装置２１００との間で予め定められた方法によって暗号を解読する。ここで暗号が正常に解読されたパケットはパケット変換手段２２０６に出力され、暗号の解読が正常に行われなかったパケット、及びゲートウェイ装置２１００以外から受け取ったパケットは破棄される。

【０１０８】パケット変換手段２２０６は、暗号の解読されたパケットのデータ部分から、ゲートウェイ装置２１００を介してＶＴＲ２５００から受信したパケットを取り出す。またパケット変換手段２２０６は、実施の形態１におけるゲートウェイ装置１１００のパケット変換手段１１０４と同様に代理サーバ機能を持つ。従ってパケット変換手段２２０６は、暗号解読手段２２０５から受け取ったパケットのデータ部分より取り出したパケットに対して、ＩＰアドレスの付け替えを行ってパケット送信手段２２０１に与える。パケット送信手段２２０１は受け取ったパケットを、インターネット２７００を介してインターネット端末２３００に送信する。

【０１０９】このようにして、インターネット２７００に接続されたインターネット端末２３００と、プライベート・ネットワーク２６００に接続されたＶＴＲ２５００との間で通信が可能となる。即ちインターネット端末２３００がＶＴＲ２５００の動作制御等を行うことができる。これにより、例えば家の外から家庭内にあるＶＴＲの録画予約や予約状況の確認等を行うことができる。

【０１１０】以上に示したゲートウェイ装置２１００と接続サーバ装置２２００は、従来使用されているファイア・ウォールの機能を発揮しているものと考えることができる。即ち、ファイア・ウォールにおけるプライベート・ネットワーク２６００側の機能をゲートウェイ装置２１００で実現し、インターネット２７００側の機能を接続サーバ装置２２００で実現している。これは両者の間をインターネットを使用した仮想プライベート・ネットワークで接続したものと考えることができる。

【０１１１】またゲートウェイ装置２１００と接続サーバ装置２２００の間を暗号化されたパケットで通信を行い、更にゲートウェイ装置２１００は接続サーバ装置２２００から送信されたパケットのみを受信し、プライベート・ネットワーク２６００に転送することにより、接続サーバ装置２２００において高いセキュリティを確保している。そしてゲートウェイ装置２１００の処理負荷を軽減し、且つインターネット２７００とプライベート・ネットワーク２６００との相互通信を可能にしている。

【０１１２】ここで、セキュリティの強さは接続サーバ装置２２００の認証手段２２０４によって決まるので、必要に応じて新しく、又は強固なものに更新することができる。このため、ゲートウェイ装置２１００の置き換えや機能の更新等を行うことなく、ゲートウェイ装置及びプライベート・ネットワークのセキュリティの強化が確保される。

【０１１３】更に接続サーバ装置２２００は、ゲートウェイ装置２１００と同等の機能を有する他の複数のゲートウェイ装置に対して、同様の機能を発揮することができる。このような場合、接続サーバ装置２２００のセキュリティを強化することで、多数のゲートウェイ装置及びプライベート・ネットワークのセキュリティを強化することができる。このことは夫々のゲートウェイ装置のセキュリティを強化する場合に比べて、効率的かつ迅速な対応ができることを意味する。

【０１１４】なお、インターネット端末２３００が、予め接続サーバ装置２２００のＩＰアドレスを知っていれば、接続先の問い合わせを行わずに、接続サーバ装置２２００に対して直接認証要求を行うことができる。またこのような場合、ゲートウェイ装置２１００のインターネット２７００側のＩＰアドレスが動的な割り当てにより変化する場合でも、上記と同等の機能を確保することができる。更には、ゲートウェイ装置２１００のＩＰアドレスが、インターネットに接続された機器に知られることがないため、より高いセキュリティが確保される。

【０１１５】上記のような夫々装置の動作に加えて、接続サーバ装置２２００のパケット変換手段２２０６がＷｅｂサーバの機能を持つ場合、インターネット端末２３００によって送信されたパケットをゲートウェイ装置２１００に転送するのではなく、このＷｅｂサーバによって処理されて生成されたパケットを、ゲートウェイ装置２１００に直接送信することもできる。このような場合、認証手段２２０４によってプライベート・ネットワーク２６００へのアクセスを許可されたインターネット端末２３００は、パケット変換手段２２０６のＷｅｂサーバにアクセスして、ＶＴＲ２５００に要求する動作に対応する入力や選択等を行うことができる。

【０１１６】この場合、Ｗｅｂサーバ２８００は入力を処理し、ＶＴＲ２５００への動作制御を行うためのパケットを生成し、暗号化手段２２０３に出力する。パケット変換手段２２０６によって生成されたパケットは、上記と同様に暗号化されてゲートウェイ装置２１００に送信され、ゲートウェイ装置２１００で暗号を解読されてＶＴＲ２５００に送信される。またＶＴＲ２５００から送信された応答は、パケット変換手段２２０６のＷｅｂサーバによって受け取られる。この応答を受けたＷｅｂサーバはＷｅｂページの更新を行うことによって、ＶＴＲ２５００から受け取った応答をインターネット端末２３００に提示することができる。

【０１１７】このように接続サーバ装置２２００のパケット変換手段２２０６がＷｅｂサーバ機能を持つことによって、インターネット端末２３００はＶＴＲ２５００の動作制御を直接行う必要がなくなる。このため、イン

ターネット端末２３００には、ＶＴＲ２５００を制御するための専用のソフトウェアを用意しなくても、汎用のブラウザ等によってＶＴＲ２５００の動作制御が可能となる。

【０１１８】

【発明の効果】以上のように本発明によれば、プライベート・ネットワークに設置するゲートウェイ装置の処理負担を小さくし、かつプライベート・ネットワークのセキュリティを確保した上で、プライベート・ネットワークとインターネットの相互接続が可能となる。

【０１１９】さらにはゲートウェイ装置に実装される機能の追加や更新を行わなくても、接続サーバ装置側での認証機能を更新したり追加することによって、プライベート・ネットワークのセキュリティの強化が可能になるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の実施の形態１におけるゲートウェイ装置、接続サーバ装置、インターネット端末の接続関係（ネットワークシステム）を示す説明図である。

【図２】実施の形態１におけるゲートウェイ装置の構成を示すブロック図である。

【図３】実施の形態１における接続サーバ装置の構成を示すブロック図である。

【図４】実施の形態１におけるインターネット端末の構成を示すブロック図である。

【図５】本発明の実施の形態２におけるゲートウェイ装置、接続サーバ装置、インターネット端末の接続関係（ネットワークシステム）を示す説明図である。

【図６】実施の形態２におけるゲートウェイ装置の構成を示すブロック図である。

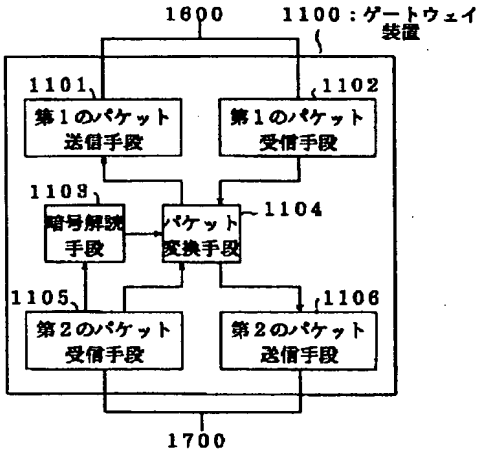
【図７】実施の形態２における接続サーバ装置の構成を示すブロック図である。

【図８】実施の形態２におけるインターネット端末の構成を示すブロック図である。

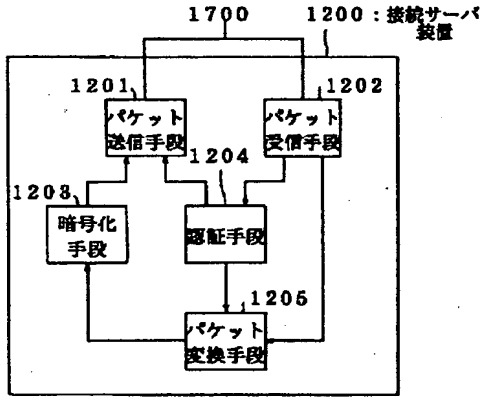
【符号の説明】

１１００，２１００　ゲートウェイ装置
１１０１，２１０１　第１のパケット送信手段
１１０２，２１０１　第１のパケット受信手段
１１０３　暗号解読手段
１１０４，２１０４　第１のパケット変換手段
１１０５，２１０５　第２のパケット受信手段
１１０６，２１０７　第２のパケット送信手段
１２００，２２００　接続サーバ装置
１２０１，２１０１　第３のパケット送信手段
１２０２，２２０２　第３のパケット受信手段
１２０３　暗号化手段
２１０５　第１の暗号化手段
２２０３　第２の暗号化手段
１２０４，２２０４　認証手段
１２０５，２２０６　第２のパケット変換手段
１３００，２３００　インターネット端末
１３０１，２３０１　第４のパケット送信手段
１３０２，２３０２　第４のパケット受信手段
１３０３，２３０３　パケット生成手段
１３０４，２３０４　認証要求手段
１４００，２４００　ＰＣ
１５００，２５００　ＶＴＲ
１６００，２６００　プライベート・ネットワーク
１７００，２７００　インターネット
１８００，２８００　Ｗｅｂサーバ
２１０３　第１の暗号解読手段
２２０５　第２の暗号解読手段

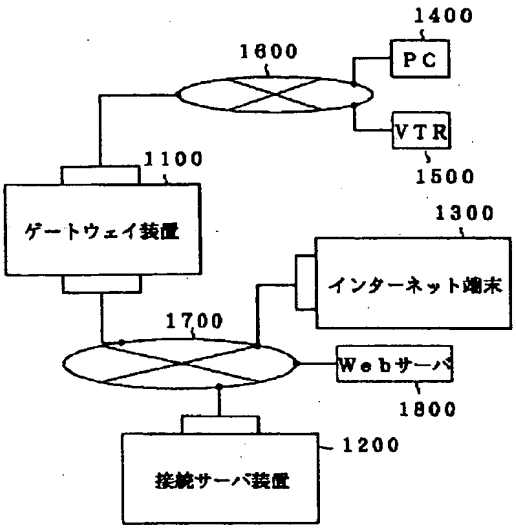
【図２】



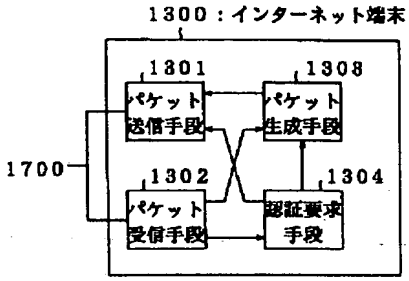
【図３】



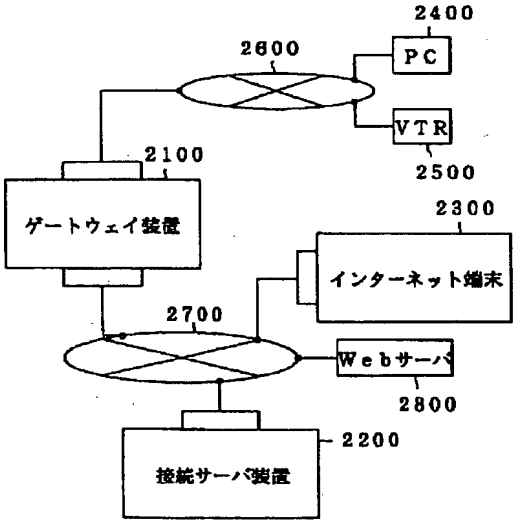
【図1】


1400
PC
1600
VTR
1500
1100
ゲートウェイ装置
1300
インターネット端末
1700
Webサーバ
1800
1200
接続サーバ装置

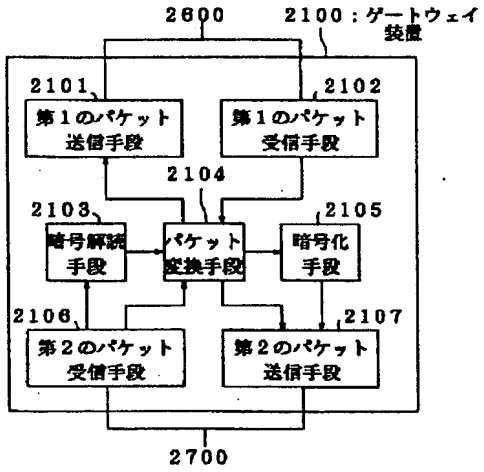
【図4】


1300：インターネット端末
1301
パケット送信手段
1308
パケット生成手段
1700
1302
パケット受信手段
1304
認証要求手段

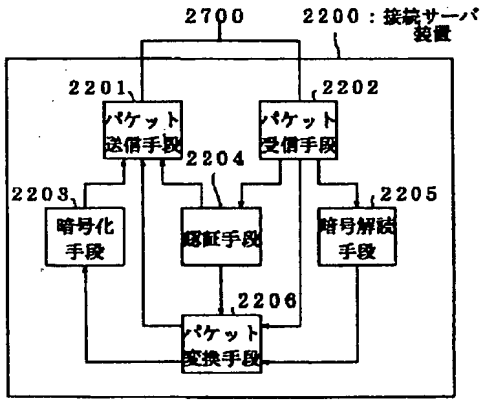
【図5】


2400
PC
2600
VTR
2500
2100
ゲートウェイ装置
2300
インターネット端末
2700
Webサーバ
2800
2200
接続サーバ装置

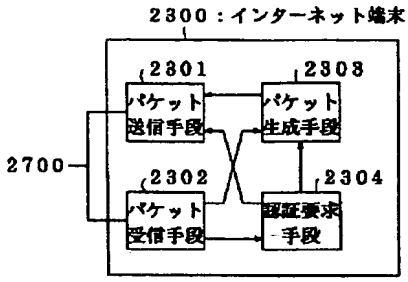
【図6】


2600
2100：ゲートウェイ装置
2101
第1のパケット送信手段
2102
第1のパケット受信手段
2104
2103
暗号解読手段
パケット変換手段
2105
暗号化手段
2106
第2のパケット受信手段
2107
第2のパケット送信手段
2700

【図7】


2700
2200：接続サーバ装置
2201
パケット送信手段
2202
パケット受信手段
2204
2203
暗号化手段
認証手段
2205
暗号解読手段
2206
パケット変換手段

【図8】


2300：インターネット端末
2301
パケット送信手段
2303
パケット生成手段
2700
2302
パケット受信手段
2304
認証要求手段